Nestor Nestor Diculescu Kingston Petersen
ATTORNEYS & COUNSELORS

Legal & Tax

Chambers Winner Europe 2022

Chambers Winner Europe 2021

Romanian DPA Report - A Year in Review - 2021

1 August 2022

Romanian DPA case studies – our top 5 picks

1

Unlawful use of body cams

Case study: A municipality implemented a bodycam system to be used by local policemen, amongst others, to discourage unlawful acts, to protect themselves against untrue accusations, as well as to protect others. The Romanian DPA decided that legal grounds indicated by the controllers do not cover the use of bodycams and that the principle of lawfulness, fairness and transparency was not observed. *(page 62-63 of the Report)*

Why it is important: *The existence of an adequate legal ground under art. 6 GDPR and the observance of data protection principles under art. 5 GDPR must be ensured by any controller, even if it is a public authority*.

2

Biometric timekeeping

Case study: A controller has processed the biometric data (fingerprints) of approx. 500 employees, who represent 1/3 from the total number of personnel. The Romanian DPA considered that such data are not adequate, relevant and limited to what it is necessary in relation to the purposes for which they are processed (data minimization principle), since the purpose declared by the controller (i.e., access and timekeeping of employees) may be attained through means which are less intrusive for the private life of employees. *(pages 78-79 of the Report)*

Why it is important: *The Romanian DPA maintains its approach that we have already witnessed in the past, as the authority is rather reluctant on using employee biometrics for access and timekeeping. From the case study, it appears that the authority has taken into consideration not only the sensitive nature of the data, but also the envisaged purpose of the processing, the total number of data subjects and their proportion as compared to the total number of employees.*

3 Documents comprising personal data disclosed on TV

Case study: An *ad-interim* hospital manager has disclosed a number of aspects regarding the clinical studies involving patients with psychiatric illnesses. Thus, during a TV program, the hospital manager has used certain documents in front of the cameras in a manner which allowed video capturing of personal data. The Romanian DPA considered that the hospital manager did not indicate which is the legal ground for using such documents comprising personal data in this context, since conducting the interview would have been possible without disclosing personal data. *(page 83 of the Report)*

Why it is important: *The Romanian DPA seems to have a broad interpretation of the material scope of GDPR. Thus, this case study seems to suggest that the GDPR protection is offered by the Romanian DPA not only to filing system-related personal data when the processing is done using non-automated means. There is no information that the data from the documents disclosed by the hospital manager were part or were intended to form part of a filing system.*

4 Deletion of signature from documents

Case study: A public person addressed a request to an educational establishment. An electronic publication asked the establishment to provide information on such public person, based on the legislation on free access to information of public interest. As a response, the establishment delivered to the publication the request of the public person in its entirety, without anonymizing any of the personal data contained therein (including the home address and the signature). According to the Romanian DPA, the document containing the request of the public person ought to have been provided with the deletion of the personal data, including the home address and the signature. *(page 85 of the Report)*

Why it is important: *The optic of the authority appears to be that the protection of the signature as personal data must not be neglected. The data protection requirements apply to the signature as well, so that, to the extent it is not necessary for a specific processing (in this case, for a disclosure), it must be excluded from the scope.*

5

Information which makes a person identifiable

Case study: A person has complained on the unlawful processing of the personal data of her daughter, placed in a foster care center (Romanian: *centru de plasament*). The Romanian DPA found that the foster care center-coordinating authority, through its answer provided to a local newspaper, disclosed personal data which may lead to the identification of the plaintiff's daughter. Thus, according to the Romanian DPA, the elements included in such answer (the date when the minor was placed in the foster care center, information about paternity, information on the center and on the period when she stayed in the center, information on diagnosis, the number of the letter whereby the police was informed on the criminal offence committed with respect to such minor) represent information which make a natural person identifiable. *(page 96 of the Report)*

Why it is important: *This is a good illustration of the fact that the name is not always necessary in order to make a person identifiable so as to qualify the information as "personal data". Even in the absence of unique identifiers, the available information may be sufficient to understand to whom it refers*.

Statistics on complaints, notices (Romanian: *sesizări*) and data breach notifications received by the authority

I.

Statistics

- **4634 complaints** received *(as compared to 5082 complaints in 2020)*;
- based on them, **319 investigations** were opened *(as compared to 296 investigations in 2020)*, resulting in:
  - **15 fines**, out of which 14 fines based on GDPR totally amounting to RON 141,530.1 (equivalent of EUR 28,700) and one fine based on ePrivacy Law 506/2004 amounting to RON 10,000 – approx. EUR 2,000, *(in 2020, there were 20 fines applied, out of which 18 based on GDPR totally amounting to RON 220,096,45 (the equivalent of EUR 45,500) and 2 fines based on Law 506/2004 totally amounting to RON 20,000 – approx. EUR 4,000)*;

- **71 reprimands** *(as compared to 55 reprimands in 2020)*;
- **40 corrective measures** *(as compared to 47 corrective measures in 2020)*;

› **171 notices** and **201 data breach notifications** received *(as compared to 204 notices and 194 data breach notifications in 2020)*;

› based on them, **372 investigations** were opened *(as compared to 398 investigations in 2020)*, resulting in:

- **21 fines** totally amounting to EUR 46,750 *(as compared to 9 fines in 2020 totally amounting to RON 652,019.5 – approx. EUR 139,000)*;
- **22 reprimands** *(as compared to 9 reprimands in 2020)*;
- **16 corrective measures** *(as compared to 18 corrective measures in 2020)*;
- **1 warning**.

› in total: **5,006 complaints**, **notices** and **data breach notifications** received *(as compared to 5480 in 2020)*;

› based on them, **691 investigations** were opened *(as compared to 694 investigations in 2020)*, resulting in:

- **36 fines** totally amounting to RON 371,131.95 – approx. EUR 63,500 *(as compared to 29 fines in 2020, totally amounting to RON 892,115.95 – approx. EUR 188,500)*;
- **93 reprimands** *(as compared to 64 reprimands in 2020)*;
- **56 corrective measures** *(as compared to 65 corrective measures in 2020)*;
- **1 warning**.

II. The most frequent cases of complaints

→ Violation of rights of data subjects, especially the right of access, right to object and right to erasure;

→ Processing of personal data through the video monitoring systems installed by employers at the workplace and by owners associations;

→ Disclosure of data on internet, including social networks;

→ Processing of data with a wrong legal ground or without legal ground;

- Violation of security measures and confidentiality rules;
- Sending unsolicited commercial communications via e-mail and phone.

III. The most frequent cases of notified data breaches

- Confidentiality/availability/integrity of data affected as a result of the unauthorized disclosure or as a result of a malicious software (ransomware type);
- Unlawful access to personal data of clients from the banking system;
- Unlawful access to video monitoring systems (CCTV);
- Disclosure of data in the healthcare system.

IV. The most frequent cases of notices

- Violation of rights and principles under GDPR;
- Disclosure of personal data without consent of data subjects;
- Publishing/disclosing personal data in online, especially on social networks;
- Processing of images using video monitoring systems;
- Sending unsolicited commercial communications;
- Violation of security measures and confidentiality rules by failure to adopt the adequate security measures on the protection of data;
- Reporting the data to the Credit Bureau.

Other statistics

- **941 requests** received for points of view on matters related to the protection of personal data *(as compared to 1151 requests in 2020)*;
- **68 legislative drafts** on which the Romanian DPA issued its notice *(as compared to 65 legislative drafts in 2020)*;
- **26 cases pending before the Court of Justice of European Union** in which Romanian DPA has issued its opinion *(as compared to 15 cases in 2020)*;
- **152 files pending in court dealt by the Romanian DPA** *(as compared to 127 files in 2020)*, out of which:
  - **25 new claims** (as compared to 29 new claims in 2020);
  - **6 claims** against acknowledging/sanctioning minutes of the Romanian DPA *(in 2020, from 29 new claims, 12 were against such minutes)*;
- **15 preliminary complaints** received by the Romanian DPA from persons unsatisfied by the answer of this authority; in the context of the administrative dispute resolution procedure; 8 of such preliminary complaints were accepted *(in 2020, 18 preliminary complaints were received and 8 were accepted)*;
- **40 multinational companies** made requests analyzed by the Romanian DPA for the approval of binding corporate rules - BCRs *(as compared to 69 companies in 2020)*.

The press release is available **here** and the 2021 Annual Report is available **here** (both available only in Romanian).